

# Sleaford U3A Data Protection Policy

## **SCOPE OF THE POLICY**

This policy applies to the work of Sleaford U3A (hereafter 'the U3A'). The policy sets out the requirements that the U3A has to gather personal information for membership purposes. The policy details how personal information will be gathered, stored and managed in line with data protection principles and the General Data Protection Regulation. The policy is reviewed on an ongoing basis by the U3A committee members to ensure that the U3A is compliant. This policy should be read in tandem with the U3A's Privacy Policy.

## **WHY THIS POLICY EXISTS**

This data protection policy ensures that the U3A:

- Complies with data protection law and follows good practice.
- Protects the rights of members.
- Is transparent about how it stores and processes members data.
- Takes all possible steps to protect itself from the risks of a data breach.

## **GENERAL GUIDELINES FOR COMMITTEE MEMBERS AND GROUP LEADERS**

- The only people able to access data covered by this policy should be those who need to communicate with or provide a service to the members of the U3A.
- Data should not be shared informally among members or outside of the U3A.
- The U3A will provide induction training to committee members and group leaders to help them understand their responsibilities when handling personal data.
- Committee Members and group leaders should keep all data secure, by taking sensible precautions and following the guidelines below.
- The nominated Data Processors are the Membership Coordinator and the Beacon Administrator.
- The U3A committee will be the Data Controller - all committee members and group leaders are data custodians. However, the committee will nominate a member (the Chair) to act on its behalf. See secure procedures.
- The U3A will provide regular updates to the committee and group leaders on their responsibilities when handling personal data.
- Strong passwords must be used and they should never be shared.
- Personal data should not be shared outside of the U3A unless with prior consent and/or for specific and agreed reasons.
- Member information should be reviewed and consent refreshed periodically via the membership renewal process or when policy is changed.
- The U3A should request help from The Third Age Trust if they are unsure about any aspect of data protection.

## **DATA PROTECTION PRINCIPLES**

The General Data Protection Regulation identifies 8 data protection principles.

- Principle 1 - Personal data shall be processed lawfully, fairly and in a transparent manner
- Principle 2 - Personal data can only be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purpose.
- Principle 3 - The collection of personal data must be adequate, relevant and limited to what is necessary compared to the purpose(s) data is collected for.
- Principle 4 – Personal data held should be accurate and, where necessary, kept up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate are erased or rectified without delay.
- Principle 5 – Personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed

solely for the archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

- Principle 6 - Personal data must be processed in accordance with the individuals' rights.
- Principle 7 - Personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- Principle 8 - Personal data cannot be transferred to a country or territory outside the European Union unless that country or territory ensures an adequate level of protection for the rights and freedoms of individuals in relation to the processing of personal data.

### **Lawful, fair and transparent data processing**

The U3A requests personal information from potential members and members for the purpose of sending communications about their involvement with the U3A. The forms used to request personal information will contain a privacy statement informing potential members and members as to why the information is being requested and what the information will be used for. The lawful basis for obtaining member information is due to the contractual relationship the U3A has with individual members. Members will be asked to provide consent for their data to be held and a record of this consent along with member information will be securely held. U3A members will be informed that they can, at any time, remove their consent and will be informed as to who to contact should they wish to do so. Once a U3A member requests not to receive certain communications this will be acted upon promptly and the member will be informed as to when the action has been taken.

### **Processed for Specified, Explicit and Legitimate Purposes**

Members will be informed as to how their information will be used and the Committee of the U3A will seek to ensure that member information is not used inappropriately. The U3A will ensure that group leaders are made aware of what would be considered appropriate and inappropriate communication. Inappropriate communication would include sending U3A members marketing and/or promotional materials from external service providers. The U3A will ensure that members' information is managed in such a way as to not infringe an individual members rights.

### **Adequate, Relevant and Limited Data Processing**

Members of the U3A will only be asked to provide information that is relevant for membership purposes. See Privacy Policy.

Where additional information may be required, such as health-related information, this will be obtained with the specific consent of the member who will be informed as to why this information is required, the purpose that it will be used for and will only be kept for as long as is necessary.

There may be occasional instances where a members' data needs to be shared with a third party due to an accident or incident involving statutory authorities. Where it is in the best interests of the member or the U3A.

### **Accuracy of Data and Keeping Data up to Date**

The U3A has a responsibility to ensure members' information is kept up to date. See Privacy Policy.

### **Accountability and Governance**

The U3A Committee are responsible for ensuring that the U3A remains compliant with data protection requirements and can evidence that it has. For this purpose, those from whom data is required will be asked to provide written consent. The evidence of this consent will then be securely held as evidence of compliance. The U3A Committee shall ensure that new members joining the Committee receive an induction into how data protection is managed within the U3A and the reasons for this. Committee Members shall also stay up to date with guidance and practice within the U3A movement and shall seek

additional input from the Third Age Trust should any uncertainties arise. The Committee will review data protection and who has access to information on a regular basis as well as reviewing what data is held.

### **Secure Processing**

The committee members of the U3A have a responsibility to ensure that data is both securely held and processed, using password protection or secure cloud systems when sharing data between committee members and/or group leaders. The U3A committee will be the Data Controller - all committee members and group leaders are data custodians. However, the committee will nominate a member (the Chair) to act on its behalf. A list of which members have access to what data is available from the Beacon Administrator

The U3A has contracted for services from with the following 3rd party data processors:

- U3A Beacon Administration System (Third Age Trust)
- U3A Sitebuilder, website provider (Third Age Trust)
- Go Daddy – website domain provider
- Email provider

If a third party supplier is used the committee would scrutinise the Terms and Conditions of each supplier and judge that they are GDPR compliant.

### **Subject Access Request**

U3A members are entitled to request access and / or deletion of their personal information which is held by the U3A. The request needs to be received in a written format sent to the Chairperson of the U3A. On receipt of the request, it will be formally acknowledged and dealt with within 14 days unless there are exceptional circumstances as to why the request cannot be granted. The U3A will provide a response in written format detailing all information held on the member. A record shall be kept of the date of the request and the date of the response. See Appendix A.

### **Data Breach Notification**

Were a data breach to occur action shall be taken to minimise the harm by ensuring all committee members are aware that a breach had taken place and how the breach had occurred. The committee shall then seek to rectify the cause of the breach as soon as possible to prevent any further breaches. The Chair of the U3A shall contact Third Age Trust within 24 hours of the breach occurring to notify of the breach. A discussion would take place between the Chair and Third Age Trust as to the seriousness of the breach, action to be taken and, where necessary, the Information Commissioner's Office would be notified. The committee shall also contact the relevant U3A members to inform them of the data breach and actions taken to resolve the breach.

If a U3A member contacts the U3A to say that they feel that there has been a breach by the U3A, a committee member will ask the member to provide an outline of their concerns. If the initial contact is by telephone, the committee member will ask the U3A member to follow this up with an email or a letter detailing their concern. The concern will then be investigated by members of the committee who are not in any way implicated in the breach. Where the committee needs support or if the breach is serious they should notify Third Age Trust. The U3A member should also be informed that they can report their concerns to Third Age Trust if they don't feel satisfied with the response from the U3A. Breach matters will be subject to a full investigation, records will be kept and all those involved notified of the outcome.

Policy review date: May 2021